Dokumentation
Gruppe 4 – Kaiser, Gruss

Einrichten eines SQUID – Proxyservers

Gruppe 4 / g4.loc
Server / rdf.loc = gateway0406 192.168.99.117
Subserver / g4.loc = 192.168.4.1 (pc08)
Client / g4.loc = 192.168.4.2 (pc09)

1. Geschichte von Squid:

Der Ursprung für den Squid Proxyserver ist das Harvest-Projekt, das bis zur Version 1.4 von Peter B. Danzig und Duane Wessels entwickelt wurde. Harvest wurde ab Version 2.0 von Danzig kommerziell weiterentwickelt, während Wessels aus den gleichen Harvest-Quellen den freien Squid entwickelte.

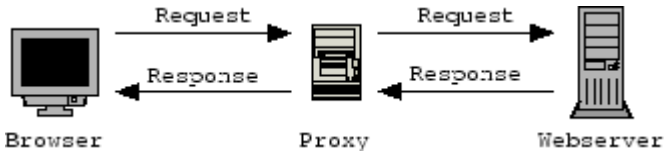
Die erste Version von Squid 2 erschien am 29. September 1998. Im Oktober 1998 bereits die Version 2.1.
Durch die kontinuierliche Entwicklungsarbeit des Teams um Duane Wessels erschienen bis Dezember 2001 fünf Versionen, in jeweils ca. 2-7 Subversionen (*Stable* genannt). D.h. etwa alle 3-4 Monate erschien eine neue Stable-Version.

Die Testphase einer neuen Version bis zum Erscheinen der ersten offiziellen Stable-Version betrug dabei je nach Version etwa 3-12 Monate.

2. Definition eines Proxyservers:

Squid ist ein WWW- und FTP-Proxy. Der Vorteil eines Proxies liegt nicht nur darin, Anfragen (für mehrere Benutzer) zu cachen, sondern auch darin, daß Clientrechner im lokalen Netz nicht unbedingt echten Internetzugriff (über Masquerading) haben müssen, was die Übersicht und die Sicherheit erhöht.

Squid gehört nicht zu den Programmen, die die CPU stark belasten, es benötigt allerdings viel Arbeitsspeicher und Platz auf der Festplatte. Zu empfehlen sind deshalb eine schnelle Festplatte und viel RAM.



3. Installation des Squid-Proxyservers:

Die Installation ist nur am **SubServer** notwendig:

apt-get install squid

oder

bei http://www.squid-cache.org herunterladen und wie folgt am Beispiel der Version 2.4 installieren:

gzip -dc squid-2.4.tar.gz | xvf -

Das Verzeichnis mit dem Namen"squid-2.4" wird angelegt und der Quellcode in das Verzeichnis "source" kopiert. Wechseln Sie in das neue Verzeichnis.

cd squid-2.4/source

Nun kann mit der Kompilierung und der Installation begonnen werden:

./configure
make
make install
make clean

4. Konfiguration des Squid-Proxyservers

Die Konfiguration erfolgt am **SubServer** in der Datei **/etc/squid/squid.conf**

Es wird eine neue Access Control List (acl) in folgendem Bereich eingetragen:

#ACCESS CONTROLS hinter acl CONNECT method CONNECT

acl g4 src 192.168.4.0/255.255.255.0

Weiterhin muss zwischen der Zeile:

#And finally deny all other access to this proxy **und** http_access deny all die Zeile

http_access allow g4

eingetragen werden

Die folgende Seite zeigt die

squid.conf

ohne ausdokumentierte Information (da Sie sonst über 4000 Zeilen lang wäre)

```
http_port 3128

hierarchy_stoplist cgi-bin ?

acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY

acl apache rep_header Server ^Apache
broken_vary_encoding allow apache

access_log /var/log/squid/access.log squid

hosts_file /etc/hosts

refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443          # https
acl SSL_ports port 563          # snews
acl SSL_ports port 873          # rsync
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl Safe_ports port 631         # cups
acl Safe_ports port 873         # rsync
acl Safe_ports port 901         # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
acl g4 src 192.168.4.0/255.255.255.0

http_access allow manager localhost
http_access deny manager

http_access allow purge localhost
http_access deny purge

http_access deny !Safe_ports

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

http_access allow localhost

http_access allow g4
http_access deny all
http_reply_access allow all
icp_access allow all

cache_effective_group proxy

coredump_dir /var/spool/squid
```

Einstellung:	**Erklärungen:**
http_port	Port, auf dem http-Anfragen empfangen werden. Verwendet wird auch der Port 8080. Default: 3128
hierarchy_stoplist cgi-bin ?	Seiten im cgi-bin Format (Dynamische Seiten) werden direkt geladen und aus dem eigenem Cache gelöscht.
acl …	Mit "access controls" (acl) werden Listen erstellt, in der die Zugriffe auf den Proxy bestimmt werden. Hierbei ist folgendes zu beachteten. Als erstes muss ein acl definiert werden. acl rechner_1 src 192.168.99.1 Der ACL-Name "rechner_1" ist hier die IP "192.168.99.1" zugewiesen worden. Die Abkürzung "src" verweist auf eine IP-Adresse. Weitere Abkürzungen können aus der Konfigurationsdatei entnommen werden. Nach der Definition werden die Rechte bestimmt. http_access allow rechner_1 Der Client mit dem ACL-Name"rechner_1" wird der Zugriff auf Internetseiten eingeräumt. Bei der Freigabe ist folgendes zu beachten: Es ist alles erlaubt, wenn einzelnes verboten ist. Es ist, alles verboten, wenn einzelnes erlaubt ist. Eine Verwendung von "Allow" und "Deny" ist nicht zulässig.
Refresh_pattern ^ftp: refresh_pattern ^gopher: refresh_pattern ^gopher:	Default Einstellungen:	refresh_pattern ^ftp: 1440 20% 10080 refresh_pattern ^gopher: 1440 0% 1440 refresh_pattern . 0 20% 4320
cache_effective_group	Läuft Squid unter Superuserrechten, wird hier die UID/GID (User Identification / Group Identification) geändert. Bei einigen Linux-Distributoren (z.B. SUSE-Linux) wird die hier verwendete Gruppe nicht verwendet. In diesen Fällen ist die default- Einstellung zu wählen. Default: nobody
cache_dir	Ort des Cacheverzeichnises. Die Abkürzung "ufs" verweißt auf das verwendete Speicherprinzip des Caches. Der erste numerische Zahlenwert gibt die maximale Größe (in MB) des Caches an. Im Cacheverzeichnis werden 16 Ordner mit jeweils 256 Unterordnern angelegt. Default: ufs /var/squid/cache 100 16 256
cache_mem	Größe des Caches im Hauptspeicher (RAM). Default: 8 MB
cache_swap_low cache_swap_high	Ist der Cache zu 95% belegt, wird dieser bis zum low-level gelöscht. Default: 90 und 95
cache_access_log	Ort der Logdatei, der erlaubten Zugriffe. Default: /var/squid/logs/access.log
cache_store_log	Ort der Logdatei, der geblockten Zugriffe. Default: /var/squid/logs/store.log
cache_mgr	In den Fehlermeldungen wird die Angegebene E-Mail angezeigt
maximum_object_size	Objekte größer dem angegebenen Wert in kb (Kilo Byte) werden nicht im Cache gespeichert.

5. Konfiguration des Clients:

...am **Client** müssen nur die Einstellungen im Browser geändert werden:

z.B.: im neuen Iceweasel Browser:

Edit >> **Preferences** >> **Advanced** >> **Network** >> **Connection** >> **Settings**

Dann Umstellen auf **Manual Proxy Configuaration** stellen und unter **HTTP Proxy** die Adresse des **Subserver** eintragen:

192.168.4.1 oder **pc08**

unter Port: **3128** (siehe Konfiguration Squid) eintragen

und die Option **Use this proxy server for all protocols** aktivieren

6. Start des Squid – Proxyservers:

Um den Proxy zu aktivieren muss auf dem **Subserver** entweder ein

/etc/init.d/squid reload

oder ein

/etc/init.d/squid restart

durchgeführt werden.

→Nun funktioniert der HTTP Zugriff auf dem **Clienten**

7. Einstellungsbeispiel: Webseiten sperren

Lege eine Datei namens **/etc/squid/gesperrt** an und stelle sicher, dass nur Root Schreibrechte darauf besitzt:

mkdir /etc/squid
touch /etc/squid/gesperrt
chmod 644 /etc/squid/gesperrt

Öffne die Datei **/etc/squid/gesperrt** mit einem Editor (z.B.: vim) und schreibe in eine Zeile ein Wort oder einen Ausdruck, der nicht in der URL vorkommen darf. Hier ein Beispiel:

Sex,
Gina,
Wild

Nun öffne wieder **/etc/squid.conf**, suche die vielen **acl** (access control list) Einträge und füge diese Zeile hinzu:

acl gesperrt url_regex -i "/etc/squid/gesperrt"

Alles zusammen könnte das also so aussehen:

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025 - 65535
acl CONNECT method CONNECT
acl gesperrt url_regex -i "/etc/squid/gesperrt"

Etwas tiefer füge die folgende Zeile zu den vielen Einträgen der Form **"http_access deny/allow acl"** hinzu:

http_access deny gesperrt

Nach jeder Änderung der Konfiguration sollte man Squid neu starten:

/etc/init.d/squid restart

Jetzt bleibt nur noch der Test ob die URLs auch wirklich gesperrt sind oder ob uns irgendwo ein Fehler unterlaufen ist (Proxyeinstellung am Clienten muss stimmen).

9. Problem aus der Praxis

→ Squid zeigt beim Starten auf dem **Subserver** keine Fehlermeldung

/etc/init.d/squid restart

→ Client baut trotz erfolgreichem restart keine Verbindung zum Web auf

Ursachenforschung mit Hilfe von Nmap (Portscanner)

→ Installation von Nmap auf dem **Clienten**

apt-get install nmap

→ Ports scannen

nmap 192.168.4.1

→ Port 3128 **nicht** aktiv / geöffnet

→ am **Subserver** die Rechtevergabe der Squid datei kontrollieren:

/var/spool/squid# ls –la

→ der Datei **swap.state** fehlen die Ausführungs / Execute Rechte

Fehlerbehebung mit Hilfe von chmod (Rechtevergabe)

→ der Datei **swap.state** die passenden Rechte geben:

chmod 770 swap.state

→ Neustart des Squid – Proxyservers

→ der Client kann eine Verbindung zum Web herstellen